

Leah's Copy
DCID NO. 1/16

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/16

SECURITY OF FOREIGN INTELLIGENCE
IN COMPUTER-CONTROLLED
DATA PROCESSING SYSTEMS AND NETWORKS

(Effective xx xxxx xxxx)

POLICY - The use of computer-controlled data processing systems and networks will in no way expose intelligence information to compromise and exploitation. The required protection, handling, and access of specific compartments of intelligence information is defined in existing policy documentation; the policy stated in this Directive and the requirements established in the accompanying Regulation are intended to enforce the same classification, compartmentation, and need-to-know now enforced for printed material. The determination of whether a data processing system or network provides the required protection will be system/network specific and the basis for making this determination will be consistent and uniform throughout the NFIB community.

Computer-controlled data processing systems and networks involving foreign governments will be addressed on a case-by-case basis by the NFIB member(s) involved.

Nothing in this Directive shall supersede or augment the requirements on the control, use, and dissemination of Restricted Data, Formerly Restricted Data, or Communications Security (COMSEC) related material as established by or under existing statutes, directives, or Presidential policy.

AUTHORITY - To insure uniformity in the protection of intelligence information, an approval authority from among the NFIB members will be explicitly designated for each data processing system/network.

Single User System/Network - The NFIB member who is the single user of a system/network is designated the Approval Authority for that system/network.

Shared System/Network - One NFIB member will be designated as the Principal Approval Authority when a system/network is jointly used by more than one NFIB member.

Concatenated Systems/Networks - When two or more systems/networks are interconnected or when a system is connected to a network of systems, each NFIB member who is already designated as the Approval Authority or Principal Approval Authority of any of the systems/networks involved will become a member of the Joint Approval Authority for the concatenated systems/networks. One of the members of the Joint Approval Authority will be designated Principal Joint Approval Authority and all NFIB members shall act as a common body for carrying out the responsibilities of the Joint Approval Authority.

RESPONSIBILITIES - The Approval Authority, Principal Approval Authority and Principal Joint Approval Authority are responsible for:

a. Assuring the most economical and effective utilization of resources while complying with the stated Policy.

b. Identifying the information protection requirements for the specific system/network based on applicable intelligence information protection policies.

c. Defining the complete set of protection measures/mechanisms required based on the functionality of the system/network, the user/operational environment, the information characteristics, and applicable intelligence information protection criteria.

d. Performing the technical assessments, risk analyses, and testing upon which an accreditation of the system/network can be based.

e. Evaluating the system/network for compliance with this directive and the standards/criteria established in the accompanying Regulation, and certifying such compliance.

f. Accrediting the system/network and defining the allowable operational environment based on the assessment and testing of the system/network.

g. Coordinating all actions to assure that all users of a data processing system/network understand and implement the decisions made.

EXEMPTIONS - The NFIB member or his designee may temporarily exempt specific systems under his jurisdiction from complete compliance with this Directive and the accompanying Regulation when such compliance would significantly impair the execution of his mission. An exemption shall be granted only when the NFIB member or his designee is absolutely confident that the other security measures in effect will adequately protect the intelligence information being processed. However, no exemption may be granted which will allow personnel with less than a TOP SECRET clearance, based on a background investigation, to access a system or network containing Sensitive Compartmented Information (SCI).

SUPERSESSSION - This Directive supersedes Director of Central Intelligence Directive No. 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks", effective 6 June 1978; and all existing directives, regulations, and other documents referencing the superseded Directive will be revised to reflect this supersession.

IMPLEMENTATION - Each NFIB member will develop and promulgate implementing directives and regulations within one year from the effective date of this Directive and the accompanying Regulation.

ADMINISTRATIVE REPORTS - Each NFIB member will provide the Director of Central Intelligence, ATTN: DCI/SECOM, an annual report as of 31 December detailing the accredited and exempted systems currently operating under his jurisdiction.

REVIEW - This Directive and the accompanying Regulation will be reviewed within three years from the effective date.

Page Denied

Next 7 Page(s) In Document Denied